PATENT
0104-0334P

IN THE U.S. PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicant: | Ulf DAHL | Conf.: | |
| Appl. No.: | New | Group: | Unassigned |
| Filed: | April 24, 2001 | Examiner: | Unassigned |
| For: | DATA SECURITY SYSTEM FOR A DATABASE (AS AMENDED) | | |

## PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, DC 20231

April 24, 2001

Sir:

The following preliminary amendments and remarks are respectfully submitted in connection with the above-identified application.

## AMENDMENTS

### IN THE TITLE OF THE INVENTION:

Please change the title of the invention to: --DATA SECURITY SYSTEM FOR A DATABASE--.

### IN THE ABSTRACT OF THE DISCLOSURE:

Please replace the Abstract of the Disclosure with the rewritten Abstract of the Disclosure located below or attached on a separate sheet attached hereto.

IN THE SPECIFICATION:

Please replace the paragraph beginning on page 1, line 3, with the following rewritten paragraph:

--The present invention relates to the technical field of computer-aided information management, and concerns more specifically a method and an apparatus for data processing for accomplishing increased protection against unauthorized processing of data.--

Please replace the paragraph beginning on page 1, line 10, with the following rewritten paragraph:

--In the field of computer-aided information management, it is strongly required that the protection against unauthorized access of data registers be increased, especially against violation of the individual's personal registers, i.e. registers containing information on individuals. In particular, there are regulations restricting and prohibiting the linking and matching of personal registers. Also in other fields, such as industry, defense, banking, insurance, etc, improved protection is desired against unauthorized access to the tools, databases, applications etc. that are used for administration and storing of sensitive information.--

Please replace the paragraph beginning on page 2, line 19, with the following rewritten paragraph:

--For a closer description of the details and advantages of this encrypting and storing method, reference is made to WO95/15628, which is to be considered to constitute part of the present description. The storing principle according to steps 1-4 above is herein referred to as PTY, which is an abbreviation of the principal of PROTEGRITY which stands for "Protection and Integrity".--

Please replace the paragraph beginning on page 2, line 31, and ending on page 3 line 11, with the following rewritten paragraph:

--In the technical field at issue, so-called shell protections are today the predominant method of protection. Shell protection comprises on the one hand the external security (premises) and, on the other hand, an authorization check system ACS with user's passwords for controlling the access. ACS is used as shell protection for main frames, client/server systems and PC, but it does not give full protection and the information at issue can often relatively easily be subjected to unauthorized access. This protection has been found more "sensitive" information is be stored, which must permit managing via distribution, storing and processing in dynamically changing environments, especially local distribution to personal computers. Concurrently with this development, the limits of the system will be more and more indistinct and the effect afforded by a shell protection deteriorates.--

Please replace the paragraph beginning on page 3, line 14, with the following rewritten paragraph:

--In view of that stated above, the object of the present invention is to provide an improved method for processing information, by means of which it is possible to increase the protection against unauthorized access to sensitive information.--

Please replace the paragraph beginning on page 3, line 19, with the following rewritten paragraph:

--A special object of the invention is to provide a technique for data processing or managing, which makes it possible for the person responsible for the system, the management of the organization etc. to easily establish and continuously adapt the user's possibility of processing stored information that is to be protected.--

Please replace the paragraph beginning on page 3, line 25, with the following rewritten paragraph:

--A further object of the invention is to provide a technique for data processing which offers protection against attempts at unauthorized data processing by means of non-accepted software.--

Please delete the paragraph beginning on page 3, line 34, and ending on line 37 in its entirety.

Please replace the paragraph beginning on page 4, line 28, with the following rewritten paragraph:

- --"Data element type" identifies a specific category of data. For example, identification information (name and address) could be particular data element type. Whereas, some descriptive information (social allowance) could be a different data element type, and other descriptive information could be yet another different data element type.--

Please replace the paragraph beginning on page 5, line 26 and ending on page 6, line 16, with the following rewritten paragraph:

--The inventive method offers a new type of protection, which differs essentially from the prior-art shell protection and which works on the cell or data element level. Each data element type used in the records in the first database is thus associated with one or more protection attributes, which are stored in a separate data element protection catalogue and which protection attributes state rules of how to process the corresponding data element values. It should be particularly noted that the calling to the data element protection catalogue is required, or in other words compelling. This means that in a system, in which the method according to the invention is implemented, a user, who for instance wants to read a certain data element value in a given record in the first database, by his attempt to access to the element value automatically produces a system calling to the data element protection catalogue in the second database for collecting the protection attributes associated with the corresponding data element types. The continued processing procedure (reading of data element value) of the system is also controlled *compellingly* in accordance with the collected protection attribute/attributes applying to the corresponding data element types.--

Please replace the paragraph beginning on page 6, line 17, with the following rewritten paragraph:

--The term "data element protection catalogue" and the use thereof according to the invention must not be confused with the known term "active dictionary", which means that, in addition to an operative database, there is a special table indicating different definitions or choices for data element values in the operative database, for instance that a data element value "yellow" in terms of definition means a color code which is within a numeric interval stated in such a reference table.--

Please replace the paragraph beginning on page 7, line 17, with the following rewritten paragraph:

--According to the invention, it is thus the individual data element (date element type) and not the entire register that becomes the controlling unit for the way in which the organization, operator etc. responsible for the system has determined the level of quality, responsibility and safety regarding the management of information.--

Please replace the paragraph beginning on page 7, line 23, with the following rewritten paragraph:

--To obtain a high level of protection, the data element protection catalogue is preferably encrypted so as to prevent unauthorized access thereto.--

Please replace the paragraph beginning on page 11, line 6, with the following rewritten paragraph:

--The hardware component 10 can as an independent unit perform at least the following functions:

- Creating variable, reversible and non-reversible encrypting algorithms for the PTY encryption and providing the algorithms with the necessary variables;
- Initiating alterations of storage identities (SID) in stored data according to PTY, on the one hand data in O-DB and, on the other hand, data in the data element protection catalogue of IAM-DB;
- Storing user authorizations having access to records in O-DB; and
- Linking original identities OID to the correct record in O-DB.--

Please replace the paragraph beginning on page 11, line 22, with the following rewritten paragraph:

--The control module 20 controls the handling of the types of data protection that the system can supply.--

Please replace the subheading beginning on page 11, line 28, with the following rewritten subheading:

--Program Module 30 (PTY-API) 30--

Please replace the paragraph beginning on page 14, line 21, with the following rewritten paragraph:

--The table, which in Fig. 4 is shown below the database IAM-DB, symbolizes an exemplifying content of the data element protection catalogue, here designated DPC. As an example, it may here be assumed that the protection function Funcl corresponds to "degree of encryption". If the descriptive information DI at issue is to be stored as a data element value DV associated with the specific data element type DT1 in the data element protection catalogue, the protection attribute "5" registered in the data element protection catalogue is collected automatically in this case. The descriptive information DI at issue will thus, automatically and compellingly, be encrypted with the strength "5" for generating an encrypted data element value DV as follows:--

Please replace the paragraph beginning on page 16, line 8, with the following rewritten paragraph:

--To increase the level of protection still more, the data element protection catalogue DPC is preferably stored in IAM-DB in encrypted form in accordance with the PTY principle, in which case for instance the data element types correspond to the above storage identity and the protection attributes correspond to the descriptive information or data element values above, as schematically illustrated in Fig. 4. This efficiently prevents every attempt at circumventing the data element protection by unauthorized access and interpretation of the content of the data element protection catalogue.--

Please replace the paragraph beginning on page 17, line 17 and ending on Page 18, line 13, with the following rewritten paragraph:

--Now assume for the purpose of illustration that Func2 in the data element protection catalogue DPC in Fig. 4 corresponds to this protection attribute and that data elements of the data element type DT1 and DT2, respectively, are only allowed to be processed with the accepted applications or programs P1 and P2, respectively. Unauthorized handling of the corresponding data elements by means of, for instance, a different program P3, or a modified version P1′ of P1, should be prevented. As protection attribute in the data element protection catalogue, data identifying P1 and P2 is therefore stored. In a preferred example, an encryptographic check sum P1* and P2*, respectively, is created, in a manner known per se, based on every accepted program P1 and P2, respectively. These check sums may be considered to constitute a unique fingerprint of the respective accepted programs, and these fingerprints can be stored as protection catalogue as illustrated schematically in Fig. 4. It should however be noted that such check sums for accepted programs can optionally be stored in a data element protection attributes in the data element protection catalogue of their own for registering of accepted programs, separately from the data element protection catalogue with protection attributes for encryption strength.--

Please replace the paragraph beginning on page 18, line 21, with the following rewritten paragraph:

--By periodic use of the above-described functionality protection, it is possible to reveal and/or prevent that an unauthorized person (for instance a "hacker") breaks into the system by means of a non-accepted program and modifies and/or adds descriptive data in such a manner that the descriptive data will then be identifying for the record. The data element values are thus not allowed to become identifying in the operative database O-DB.--

Please replace the paragraph beginning on page 20, line 10, with the following rewritten paragraph:

> --It will be appreciated that such a compelling calling to the data element protection catalogue DPC, when making an attempt at reading, may result in the attempt failing, wholly or partly, for several reasons, depending on the protection attribute at issue, which is linked to the data element value/values that is/are to be read. For instance, the attempt at reading may be interrupted owing to the user trying to use a non-accepted program and/or not being authorized to read the term involved.--

Please replace the paragraph beginning on page 20, line 25, with the following rewritten paragraph:

--Fig. 5 shows an example of a user interface in the form of a dialogue box, by means of which a person responsible for

IAM, i.e. a person responsible for security, may read and/or alter the protection attributes stated in the data element protection catalogue. In the Example in Fig. 5, the data element types "Housing allowance" and "Social allowance" have both been provided with protection attributes concerning encryption, sorting out, logging and owner. Moreover, registration of authorized users and protected programs linked to the data element type "Social allowance" has taken place in submenus.--

IN THE CLAIMS:

Please amend the claims as follows:

2. (Amended) A method as claimed in claim 1, further comprising the measure of storing the protection attribute/attributes of the data element protection catalogue (DPC) in encrypted form in the second database (IAM-DB) and, when collecting protection catalogue (DPC) effecting decryption thereof.

3. (Amended) A method as claimed in claim 1, wherein each record (P) in the first database (O-DB) has a record identifier, and wherein the method further comprises the measure of storing the record identifier in encrypted form (SID) in the first database (O-DB).

4. (Amended) A method as claimed in claim 1, wherein the encryption of data in the first database (O-DB) and/or the encryption of data in the second database (IAM-DB) is carried out in accordance with a PROTEGRITY principle with floating storage identity.

5. (Amended) A method as claimed in claim 1, wherein the protection attribute/attributes of the data element types comprise attributes stating rules for encryption of the corresponding data element values in the first database (O-DB).

6. (Amended) A method as claimed in claim 1, wherein the protection attribute/attributes of the data element types comprise attributes stating rules for which program/programs or program versions is/are allowed to be used for managing the corresponding data element values in the first database (O-DB).

7. (Amended) A method as claimed in claim 1, wherein the protection attribute/attributes of the data element values comprise attributes stating rules for logging the corresponding data element values in the first database (O-DB).

<u>NEW CLAIMS</u>:

Please add the following claims:

--9. A method for processing of confidential data comprising the steps of:

providing a first database (P-DB), a second database (O-DB), and a third database (IAM-DB);

entering descriptive information (DI) with certain portions of the descriptive information being classified as certain data types (DT) of a plurality of different data types;

assigning an initial identity (OID) to the descriptive information;

storing a first record in the first database including in the initial identity;

encrypting the initial identity to form a storage identity (SID);

accessing a catalogue (DCP) of encryption protection degrees in the third database, the catalogue including encryption levels for each of the different data types;

encrypting the certain portions of the descriptive information in accordance with their data types; and

storing a second record in the second database including the storage identity and the encrypted descriptive information (DV).

10. The method according to claim 9, wherein the first record is not encrypted.

11. The method according to claim 10, wherein the first record includes an individual's name and address.

12. The method according to claim 9, wherein the third database is physically separate from the second database.

13. The method according to claim 11, wherein the different data types represent different types of personal data corresponding to the individual.

14. The method according to claim 9, wherein said step of encrypting the initial identity to form the storage identity includes a non-reversible encryption followed by a reversible encryption.

15. The method according to claim 9, wherein the catalogue of encryption protection degrees in the third database is encrypted.

16. The method according to claim 9, wherein the catalogue of encryption protection degrees includes encryption rules for encrypting the different data types.

17. The method according to claim 9, wherein the catalogue of encryption protection degrees includes rules for which program or programs may manage the different data types.--

## REMARKS

Claims 1-17 are pending in the present application. Claims 9-17 have been added.

Entry of the above amendments is earnestly solicited. An early and favorable first action on the merits is earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact John A. Castellano (Reg. #35,094) at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By____________________________
John A. Castellano, #35,094

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

JAC/lhb
0104-0334P

Attachments

## ABSTRACT OF THE DISCLOSURE

A method and an apparatus for processing data provides protection for the data. The data is stored as encrypted data element values (DV) in records (P) in a first database (O-DB), each data element value being linked to a corresponding data element type (DT). In a second database (IAM-DB), a data element protection catalogue (DC) is stored, which for each individual data element type (DT) contains one or more protection attributes stating processing rules for data element values (DV), which in the first database (O-DB) are linked to the individual data element type (DT). In each user-initiated measure which aims at processing a given data element value (DV) in the first database (O-DB), a calling is initially sent to the data element protection catalogue for collecting the protection attribute/attributes associated with the corresponding data element types. The user's processing of the given data element value is controlled in conformity with the collected protection attribute/attributes.

## VERSION WITH MARKINGS TO SHOW CHANGES MADE

*In the Specification*:

The paragraph beginning on page 1, line 3, has been amended as follows:

--The present invention relates to the technical field of computer-aided information management, and concerns more specifically a method and an apparatus for data processing [according to the preamble to claim 1 and claim 8, *respectively*] for accomplishing increased protection against [*unauthorised*] unauthorized processing of data.

The paragraph beginning on page 1, line 10, has been amended as follows:

--In the field of computer-aided information management, it is strongly required that the protection against [*unauthorised*] unauthorized access of data registers be increased, especially against violation of the individual's personal registers, i.e. registers containing information on individuals. In particular, there are regulations restricting and prohibiting the linking and matching of personal registers. Also in other fields, such as industry, [*defence*] defense, banking, insurance, etc, improved protection is desired against [*unauthorised*] unauthorized access to the tools, databases, applications etc. that are used for administration and storing of sensitive information.

The paragraph beginning on page 2, line 19, has been amended as follows:

For a closer description of the details and advantages of this encrypting and storing method, reference is made to WO95/15628, which is to be considered to constitute part of the present description. The storing principle according to steps 1-4 above is [*below*] herein referred to as PTY, which is an abbreviation of the [*concept*] principal of PROTEGRITY which stands for "Protection and Integrity".

The paragraph beginning on page 2, line 31, and ending on page 3 line 11, has been amended as follows:

In the technical field at issue, so-called shell protections[*, however,*] are today the predominant method of protection. Shell protection comprises on the one hand the external security (premises) and, on the other hand, an [*authorisation*] authorization check system ACS with user's passwords for controlling the access. ACS is used as shell protection for main frames, client/server systems and PC, but it does not give full protection and the information at issue can often relatively easily be subjected to [*unauthorised*] unauthorized access. This protection has been found more "sensitive" information is be stored, which must permit managing via distribution, storing and processing in dynamically changing environments, especially local distribution to personal computers. Concurrently with this development, the limits of the system will be more and more indistinct and the effect afforded by a shell protection deteriorates.

The paragraph beginning on page 3, line 14, has been amended as follows:

In view of that stated above, the object of the present invention is to provide an improved method for processing information, by means of which it is possible to increase the protection against [*unauthorised*] unauthorized access to sensitive information.

The paragraph beginning on page 3, line 19, has been amended as follows:

A special object of the invention is to provide a technique for data processing or managing, which makes it possible for the person responsible for the system, the management of the [*organisation*] organization etc. to easily establish and continuously adapt the user's possibility of processing stored information that is to be protected.

The paragraph beginning on page 3, line 25, has been amended as follows:

A further object of the invention is to provide a technique for data processing which offers protection against attempts at [unauthorised] unauthorized data processing by means of non-accepted software.

The paragraph beginning on page 3, lines 34-37, has been deleted.

The paragraph beginning on page 4, lines 28 and 29, have been amended as follows:

- "Data element type" [*concerns*] identifies a specific [*type*] category of data. For example, identification information (name and address) could be particular data element type. Whereas, some descriptive information (social allowance) could be a different data element type, and other descriptive information could be yet another different data element type[*having a meaning as agreed on*].

The paragraph beginning on page 5, line 26 and ending on page 6, line 16, has been amended as follows:

The inventive method offers a new type of protection, which differs essentially from the prior-art shell protection and which works on the cell or data element level. Each data element type used in the records in the first database is thus associated with one or more protection attributes, which are stored in a separate data element protection catalogue and which protection attributes state rules of how to process the corresponding data element values. It should be particularly noted that the calling to the data element protection catalogue is required, or in other words compelling. This means that in a system, in which the method according to the invention is implemented, [*is such as to imply that*] a user, who for instance wants to read a certain data element value in a given record in the first database, by his attempt to access to the element value automatically [and compellingly] produces a system calling to the data element protection catalogue in the second database for collecting the protection attributes associated with the corresponding data element types. The continued processing procedure (reading of data element value) of the system is also controlled *compellingly* in accordance with the collected protection attribute/attributes applying to the corresponding data element types.

The paragraph beginning on page 6, line 17, has been amended as follows:

The term "data element protection catalogue" and the use thereof according to the invention must not be confused with the known term "active dictionary", which means that, in addition to an operative database, there is a special table indicating different definitions or choices for data element values in the operative database, for instance that a data element value "yellow" in terms of definition means a [*colour*] color code which is within a numeric interval stated in such a reference table.

The paragraph beginning on page 7, line 17, has been amended as follows:

According to the invention, it is thus the individual data element (date element type) and not the entire register that becomes the controlling unit for the way in which the [*organisation*] organization, operator etc. responsible for the system has determined the level of quality, responsibility and safety regarding the management of information.

The paragraph beginning on page 7, line 23, has been amended as follows:

To obtain a high level of protection, the data element protection catalogue is preferably encrypted so as to prevent [*unauthorised*] unauthorized access thereto.

The paragraph beginning on page 11, line 6, has been amended as follows:

The hardware component 10 can as an independent unit perform at least the following functions:

- Creating variable, reversible and non-reversible encrypting algorithms for the PTY encryption and providing the algorithms with the necessary variables;
- Initiating alterations of storage identities (SID) in stored data according to PTY, on the one hand data in O-DB and, on the other hand, data in the data element protection catalogue of IAM-DB;
- Storing user [authorisations] authorizations having access to records in O-DB; and
- Linking original identities OID to the correct record in O-DB.

The paragraph beginning on page 11, line 22, has been amended as follows:

The control module 20 controls the handling of the types of data protection that the system can supply.

The subheading beginning on page 11, line 28, has been amended as follows:

Program Module 30 ([P]PTY-API) 30

The paragraph beginning on page 14, line 21, has been amended as follows:

The table, which in Fig. 4 is shown below the database IAM-DB, [*symbolises*] symbolizes an exemplifying content of the data element protection catalogue, here designated [*DC*] DPC. As an example, it may here be assumed that the protection function Func1 corresponds to "degree of encryption". If the descriptive information DI at issue is to be stored as a data element value DV associated with the specific data element type DT1 in the data element protection catalogue, the protection attribute "5" registered in the data element protection catalogue is collected automatically in this case. The descriptive information DI at issue will thus, automatically and compellingly, be encrypted with the strength "5" for generating an encrypted data element value DV as follows:

The paragraph beginning on page 16, line 8, has been amended as follows:

To increase the level of protection still more, the data element protection catalogue [DC] DPC is preferably stored in IAM-DB in encrypted form in accordance with the PTY principle, in which case for instance the data element types correspond to the above storage identity and the protection attributes correspond to the descriptive information or data element values above, as schematically illustrated in Fig. 4. This efficiently prevents every attempt at circumventing the data element protection by [unauthorised] unauthorized access and interpretation of the content of the data element protection catalogue.

The paragraph beginning on page 17, line 17 and ending on Page 18, line 13, has been amended as follows:

Now assume for the purpose of illustration that Func2 in the data element protection catalogue [DC] DPC in Fig. 4 corresponds to this protection attribute and that data elements of the data element type DT1 and DT2, respectively, are only allowed to be processed with the accepted applications or programs P1 and P2, respectively. [Unauthorised] Unauthorized handling of the corresponding data elements by means of, for instance, a different program P3, or a modified version P1′ of P1, should be prevented. As protection attribute in the data element protection catalogue, data identifying P1 and P2 is therefore stored. In a preferred example, an encryptographic check sum P1* and P2*, respectively, is created, in a manner known per se, based on every accepted program P1 and P2, respectively. These check sums may be considered to constitute a unique fingerprint of the respective accepted programs, and these fingerprints can be stored as protection catalogue as illustrated schematically in Fig. 4. It should however be noted that such check sums for accepted programs can optionally be stored in a data element protection attributes in the data element protection catalogue of their own for registering of accepted programs, separately from the data element protection catalogue with protection attributes for encryption strength.

The paragraph beginning on page 18, line 21, has been amended as follows:

By periodic use of the above-described functionality protection, it is possible to reveal and/or prevent that an [unauthorised] unauthorized person (for instance a "hacker") breaks into the system by means of a non-accepted program and modifies and/or adds descriptive data in such a manner that the descriptive data will then be identifying for the record. The data element values are thus not allowed to become identifying in the operative database O-DB.

The subparagraph beginning on page 20, line 10, has been amended as follows:

> It will be appreciated that such a compelling calling to the data element protection catalogue [DC] DPC, when making an attempt at reading, may result in the attempt failing, wholly or partly, for several reasons, depending on the protection attribute at issue, which is linked to the data element value/values that is/are to be read. For instance, the attempt at reading may be interrupted owing to the user trying to use a non-accepted program and/or not being [authorised] authorized to read the term involved.

The paragraph beginning on page 20, line 25, has been amended as follows:

Fig. 5 shows an example of a user interface in the form of a dialogue box, by means of which a person responsible for IAM, i.e. a person responsible for security, may read and/or alter the protection attributes stated in the data element protection catalogue. In the Example in Fig. 5, the data element types "Housing allowance" and "Social allowance" have both been provided with protection attributes concerning encryption, sorting out, logging and owner. Moreover, registration of [authorised] authorized users and protected programs linked to the data element type "Social allowance" has taken place in submenus.

IN THE CLAIMS:

The claims have been amended as follows:

2. (Amended) A method as claimed in claim 1, further comprising the measure of storing the protection attribute/attributes of the data element protection catalogue [(DC)] (DPC) in encrypted form in the second database (IAM-DB) and, when collecting protection catalogue [(DC)] (DPC) effecting decryption thereof.

3. (Amended) A method as claimed in claim 1 [any one of the preceding claims], wherein each record (P) in the first database (O-DB) has a record identifier, and wherein the method further comprises the measure of storing the record identifier in encrypted form (SID) in the first database (O-DB).

4. (Amended) A method as claimed in claim 1 [any one of the preceding claims], wherein the encryption of data in the first database (O-DB) and/or the encryption of data in the second database (IAM-DB) is carried out in accordance with [the PTY] a PROTEGRITY principle with floating storage identity.

5. (Amended) A method as claimed in claim 1 [any one of the preceding claims], wherein the protection attribute/attributes of the data element types comprise attributes stating rules for encryption of the corresponding data element values in the first database (O-DB).

6. (Amended) A method as claimed in claim 1 [any one of the preceding claims], wherein the protection attribute/attributes of the data element types comprise attributes stating rules for which program/programs or program versions is/are allowed to be used for managing the corresponding data element values in the first database (O-DB).

7. (Amended) A method as claimed in claim 1 [any one of the preceding claims], wherein the protection attribute/attributes of the data element values comprise attributes stating rules for logging the corresponding data element values in the first database (O-DB).

Claims 9-17 have been added.

PATENT
0104-0334P

IN THE U.S. PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicant: | Ulf DAHL | Conf.: | |
| Appl. No.: | NEW | Group: | UNASSIGNED |
| Filed: | April 24, 2001 | Examiner: | UNASSIGNED |
| For: | DATA SECURITY SYSTEM FOR A DATABASE (AS AMENDED) | | |

## DRAWING CORRECTION AUTHORIZATION REQUEST

Assistant Commissioner for Patents
Washington, DC 20231

April 24, 2001

Sir:

Applicant respectfully requests the Examiner's authorization of the drawing corrections shown in red ink on the attached sheet(s) as follows:

On Fig. 3 specifically, reference numerals 10, 20, 30 and 40 have been inserted. The reference numerals find support in the specification on page 10, lines 35-36 and page 11, line 30.

No new matter has been added by these changes. Please substitute the attached Corrected Formal Drawing for the corresponding red ink drawing.

The Examiner is respectfully requested to provide a Notice of Draftspersons Patent Drawing and Review Form PTO-948 or at least acknowledgement on the record of indicating that the drawings filed along with the present application have been approved.

Appl. No. NEW

If necessary, the Commissioner is hereby authorized in this, concurrent, and further replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By______________________________
John A. Castellano, #35,094

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

JAC/lhb
0104-0334P

Attachments: One (1) red ink drawing
One (1) corrected formal drawing

(Rev. 01/22/01)

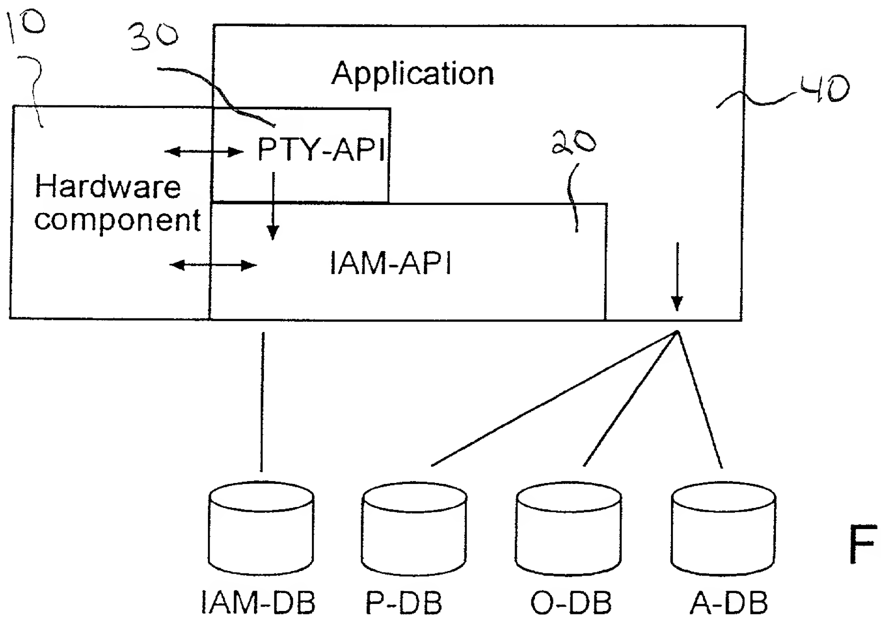
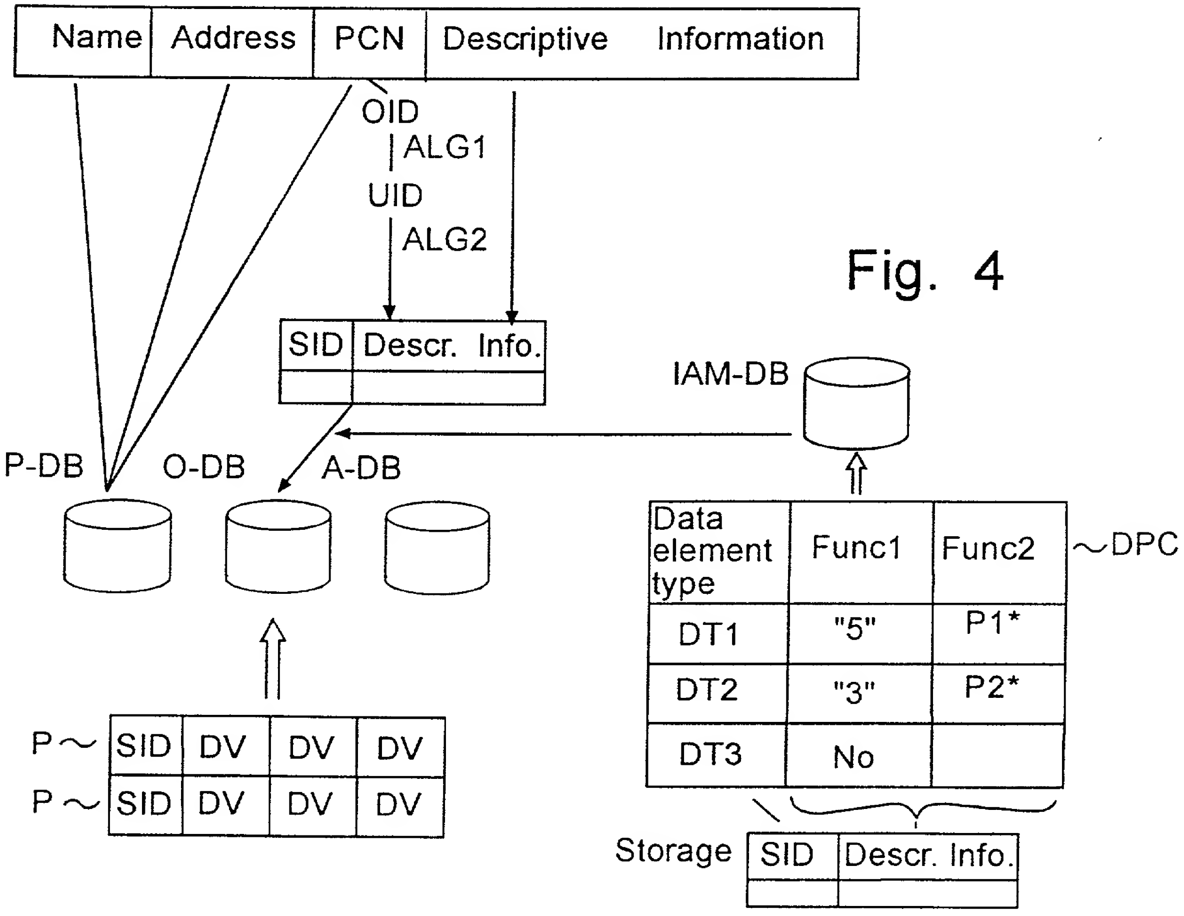


Fig. 3



| Data element type | Func1 | Func2 |
|---|---|---|
| DT1 | "5" | P1* |
| DT2 | "3" | P2* |
| DT3 | No | |

Fig. 4

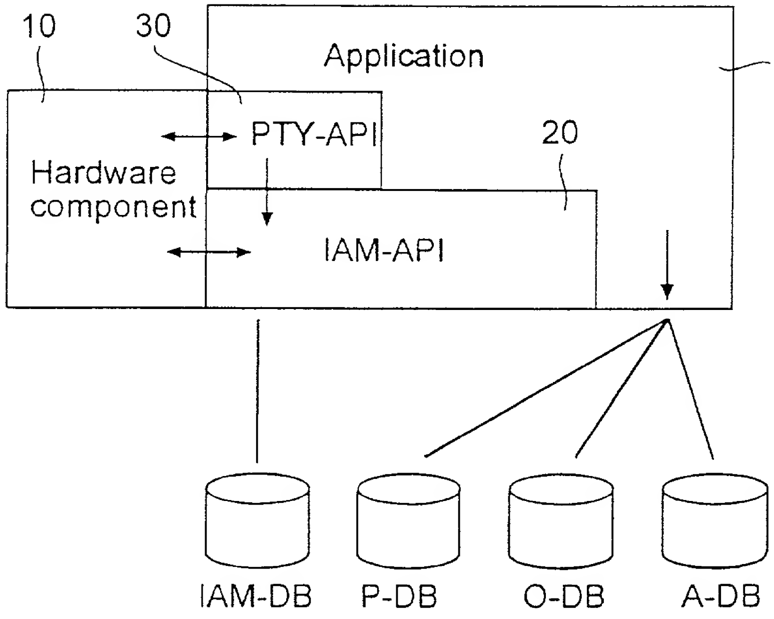
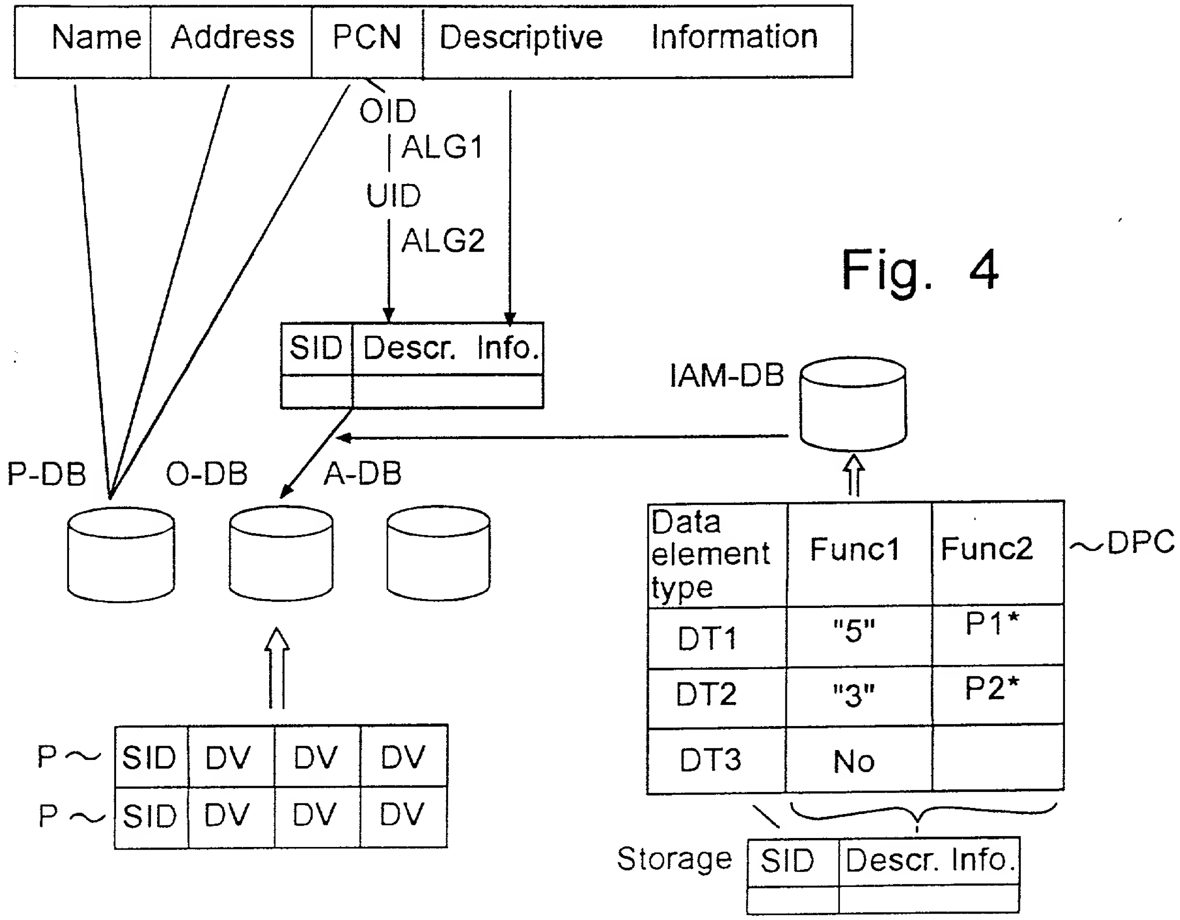


Fig. 3



| Data element type | Func1 | Func2 |
|---|---|---|
| DT1 | "5" | P1* |
| DT2 | "3" | P2* |
| DT3 | No | |

Fig. 4